Padjadjaran Journal of International Relations (PADJIR)
e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (311-333) doi: 10.24198/padjir.v1i3.26246

CYBER DIPLOMACY: MENUJU MASYARAKAT INTERNASIONAL YANG DAMAI DI ERA DIGITAL

Iskandar Hamonangan
Departemen Hubungan Internasional Universitas Indonesia, Indonesia;
email: iskandar.hamonangan91@alumni.ui.ac.id
Zainab Assegaff
Departemen Hubungan Internasional Universitas Indonesia, Indonesia;
email: zassegaff@gmail.com

Dikirim:	Direvisi:	Diterima:	Dipublikasikan:
18 Desember 2019	25 Januari 2020	28 Januari 2020	31 Januari 2020

Keywords
Diplomacy, Cyber Diplomacy, Cyber Space, Peace, International Relations

ABSTRACT
This paper aims to discuss cyber diplomacy and what it can promise to lead to a peaceful international community in the digital age. The cyber space has a special place and is a very important topic in international relations. This topic has become mainstream because most of the global actors have poured out their foreign policies and adopted various measures to pursue their strategic goals in cyberspace. This can be seen for example in the use of social media by the Ministry of Foreign Affairs to promote the country, its policies and values. However, activities in cyberspace are not always peaceful. There are two groups of countries that compete for global cyber security governance and there is competition between the United States (US) and China in fighting for cyber security. It is this conflict of interests between countries that makes cyber diplomacy necessary to mediate and prevent open cyber warfare. Cyber diplomacy is an international practice that arises from efforts to build an international cyber community, by bridging the national interests of the country and the dynamics of the world community. Therefore, the aim of cyber diplomacy is to fulfill the traditional functions of diplomacy, such as maintaining peace and building mutual trust among stakeholders, in cyberspace. This paper uses the Diplomacy theory of the School of English School to analyze what cyber diplomacy can promise for the peaceful use of cyber space. The authors argue that there are two main functions of cyber diplomacy, namely as an international communication tool to establish shared cyber norms and as an effort to minimize friction in cyberspace.

Kata Kunci
Diplomasi, Diplomasi Siber, Ruang Siber, Perdamaian, Hubungan Internasional

ABSTRAK
Makalah ini bertujuan untuk membahas mengenai diplomasi siber (*cyber diplomacy*) dan apa yang bisa dijanjikannya untuk menuju masyarakat internasional yang damai di era digital. Ruang siber telah memiliki tempat khusus dan menjadi topik yang sangat penting dalam hubungan internasional. Topik ini telah menjadi arus utama karena sebagian besar aktor-aktor

global telah menuangkan kebijakan-kebijakan luar negerinya dan mengadopsi berbagai langkah untuk mengejar tujuan-tujuan stategisnya di dalam ruang siber. Hal ini dapat dilihat misalnya pada penggunaan media sosial oleh Kementerian Luar Negeri untuk mempromosikan negara, kebijakan, dan nilai-nilainya. Namun, kegiatan di ruang siber tidak selalu damai. Terdapat dua kelompok negara yang bersaing untuk tata kelola keamanan siber global dan adanya persaingan antara Amerika Serikat (AS) dan China dalam memperebutkan keamanan siber. Konflik kepentingan antarnegara inilah yang membuat *cyber diplomacy* diperlukan untuk menengahinya dan mencegah perang siber yang terbuka. *Cyber diplomacy* adalah praktik internasional yang muncul atas upaya untuk membangun masyarakat siber internasional, dengan menjembatani antara kepentingan nasional negara dan dinamika masyarakat dunia. Oleh karena itu, tujuan dari *cyber diplomacy* adalah untuk memenuhi fungsi-fungsi tradisional diplomasi, seperti menjaga perdamaian serta membangun rasa saling percaya di antara para pemangku kepentingan, di ruang siber. Makalah ini menggunakan teori Diplomasi dari mazhab *English School* untuk menganalisis apa yang bisa dijanjikan *cyber diplomacy* bagi penggunaan ruang siber yang damai. Ada dua fungsi utama dari *cyber diplomacy*, yaitu sebagai alat komunikasi internasional untuk membangun norma siber bersama dan sebagai upaya untuk meminimalkan gesekan di ruang siber.

PENDAHULUAN

Saat ini ruang siber merupakan kenyataan yang tak terhindarkan, yang melingkupi dunia dengan jaringan yang kompleks, dan berkembang begitu cepat sehingga individu dan organisasi harus mengambil langkah-langkah yang tepat bagi keamanannya. Menurut Kim (2014), ini merupakan hal yang menantang karena masalah keamanan siber dicirikan oleh dinamika, struktur, dan aktor dalam jaringan yang kompleks, sehingga membuatnya sangat berbeda dari masalah keamanan tradisional. Kim juga berpendapat bahwa ancaman siber terus berkembang dan semakin mengaburkan batas teritorial. Ketika masalah keamanan siber terus meningkat hingga ke garis depan politik dunia, risikonya akan semakin meningkat, ketegangan dan perselisihan juga akan lebih sering terjadi (Kim, 2014, hal. 345).

Ancaman siber terus meningkat dikarenakan ketergantungan kita pada infrastruktur siber. Heffter & Goel (2018) menyatakan bahwa kemajuan teknologi modern, yang dimungkinkan oleh inovasi siber, telah memengaruhi setiap segi kehidupan, sehingga menyebabkan pemerintah, individu, dan bisnis sangat tergantung pada dunia digital agar dapat berfungsi dalam kesehariannya. Di saat yang sama, lanskap ancaman meluas dengan setiap inovasi siber, dan konsekuensi dari serangan meningkat, dari kehilangan informasi, menjadi kerugian finansial, hingga hilangnya nyawa dan harta benda (Heffter & Goel, 2018, hal. 2). Menurut mereka, negara-negara telah mengakui potensi serangan siber untuk penggunaan militer dan secara aktif mengembangkan persenjataan digital mereka, yang dapat mengarah pada perlombaan senjata siber. Hasil dari perlombaan senjata semacam ini akan meniadakan keuntungan ekonomi dan sosial dari ruang siber (Heffter & Goel, 2018, hal. 2).

Pertentangan mengenai ruang siber juga semakin rumit. Menurut Kim (2014) hal ini dikarenakan di satu sisi, terdapat dua kelompok negara yang bersaing untuk tata kelola keamanan siber global, yaitu kelompok negara-negara Barat, yang percaya bahwa internet harus lebih terbuka dan bebas, dan kelompok koalisi negara—termasuk Rusia,

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (311-333) doi: 10.24198/padjir.v1i3.26241

China, dan negara berkembang lainnya—yang percaya bahwa internet harus terorganisasi dan memiliki visi yang jelas dan lebih dikontrol oleh negara. Di sisi lain, Amerika Serikat (AS) dan China, yang merupakan dua kekuatan dunia pada abad ke-21, saling bersaing memperebutkan keamanan siber (Kim, 2014, hal. 346). Berbagai pendekatan terhadap keamanan siber dalam standar teknis, kebijakan peraturan, dan wacana keamanan sangat berbeda di antara kedua negara tersebut dan perbedaan ini cenderung menimbulkan ketegangan yang lebih luas di antara keduanya (Kim, 2014, hal. 346).

Sebelum muncul pertentangan akan tata kelola keamanan siber global, internet hanya dikelola oleh segelintir kelompok. Pada masa awalnya, tata kelola internet dilakukan oleh jaringan *multistakeholder* yang terdesentralisasi dari kelompok-kelompok masyarakat sipil, sektor swasta, pemerintah, komunitas akademik dan penelitian, serta organisasi nasional dan internasional (Kim, 2014, hal. 329). Model tata kelola *multistakeholder* ini juga disebut sebagai inisiatif *multistakeholder* (MSI) atau *multistakeholderism*, yang berupaya menyatukan para pemangku kepentingan untuk berpartisipasi dalam dialog, pengambilan keputusan, dan implementasi solusi untuk masalah dan/atau tujuan bersama. Kerangka global dari tata kelola internet didasarkan pada inisiatif dari *multistakeholder* yang sebagian besar berbasis di AS dan bukan oleh konsensus dari perwakilan pemerintah di arena diplomatik dalam organisasi internasional (Kim, 2014, hal. 329).

Contoh dari model *multistakeholder* adalah *Internet Corporation for Assigned Names and Numbers* (ICANN). ICANN merupakan organisasi non-negara yang berkantor pusat di California, AS (Kim, 2014, hal. 329). Namun, karena Departemen Perdagangan AS terus terlibat dalam persetujuan akhir untuk perubahan pada isu-isu utama, ICANN dicurigai sebagai alat hegemoni de facto AS (Mueller, 2002; 2010 dalam Kim, 2014, hal. 329). Menurut Kim (2014), Rusia, China dan negara-negara berkembang lainnya mengajukan keberatan akan ICANN. Mereka terus mengadvokasi untuk penggunaan organisasi internasional tradisional—misalnya prosedur pemungutan suara PBB—alih-alih model ICANN, dalam membuat keputusan global, dan membela hak mereka dalam mengontrol aktivitas siber domestik (Kim, 2014, hal. 330). Menurut mereka, meski kepemimpinan AS sebagai penggerak pertama ditoleransi pada tahap awal perkembangan internet, saat ini dunia harus membangun konsensus baru antarpemerintah mengenai tata kelola internet global, karena internet telah berevolusi begitu cepat sehingga negara-negara mendapati kepentingan mereka saling bertentangan (Kim, 2014, hal. 330).

Keberatan ini kemudian ditindaklanjuti dengan membawanya ke Majelis Umum PBB. Rusia mengajukan rancangan resolusi isu keamanan informasi ke Komite Pertama Majelis Umum PBB pada tahun 1998 (UNODA, t.t.). Pembahasan terus berkembang dan sejak tahun 2004 terdapat lima *Groups of Governmental Experts* (GGE) yang terus mempelajari ancaman yang ditimbulkan oleh penggunaan teknologi informasi dan komunikasi (ICT) dalam konteks keamanan internasional dan bagaimana menanganinya (UNODA, t.t.). Fokus dari GGE adalah topik-topik berikut: ancaman yang ada dan mulai muncul; bagaimana hukum internasional berlaku dalam penggunaan ICT; norma, aturan dan prinsip perilaku yang bertanggung jawab dari negara; langkah-langkah pembangunan kepercayaan; dan pembangunan kapasitas (UNODA, t.t.). Sidang GGE dilakukan secara bergantian di New York dan Jenewa dan telah bersidang sebanyak lima kali sejak tahun 2004 hingga 2017 (UNODA Fact Sheet, 2019). Sidang kelima pada tahun 2017 gagal menyepakati sidang selanjutnya. Namun, pada Desember 2018, Majelis Umum PBB membentuk GGE yang baru dan *Open-Ended Working Group* (OEWG) guna melanjutkan

sidang untuk periode 2019-2020 dan 2020-2021 (UNODA Fact Sheet, 2019).

Pertentangan yang terjadi mengenai ruang siber tentu saja bukan tanpa tujuan. Menurut Kim (2014), hal ini terjadi karena konflik kepentingan antarnegara. Ia menjelaskan, dipimpin oleh AS, negara-negara Barat berpendapat bahwa kebebasan, keterbukaan dan kepercayaan harus menjadi prinsip dasar dalam ruang siber. Mereka juga percaya bahwa berbagai aktor termasuk warga negara perorangan, masyarakat sipil, bisnis dan pemerintah harus berpartisipasi dalam penciptaan norma dan aturan internasional (Kim, 2014, hal. 331). Oleh karena itu, negara-negara Barat menggunakan siber sebagai instrumen perang untuk melawan negara lain dan tunduk pada regulasi hukum perang konvensional. Sebaliknya, negara-negara non-Barat termasuk Rusia dan China menyatakan bahwa kontrol informasi harus dimungkinkan di ruang siber untuk tujuan keamanan nasional, dan bahwa mereka tidak dapat menerima peraturan yang secara tidak adil menguntungkan negara-negara Barat (Kim, 2014, hal. 331). Oleh sebab itu, kelompok ini tidak menggunakan siber sebagai instrumen perang antarnegara.

Disimpulkan bahwa kedua kelompok negara yang bersaing ini berusaha untuk memaksimalkan kepentingan nasional mereka dalam proses pembentukan tatanan baru ruang siber. Terlepas dari apakah tantangan kelompok koalisi negara non-Barat akan berhasil, dua visi terhadap internet ini tidak akan berubah dalam waktu dekat. Dekade berikutnya akan diisi dengan pertentangan serupa (Kim, 2014, hal. 332). Oleh karena itu, perlu dilakukan *cyber diplomacy* untuk menyelaraskan kepentingan negara-negara dan agar tidak terjadi perang siber yang terbuka.

PERTANYAAN UTAMA

Pertentangan kepentingan negara-negara dalam ruang siber merupakan hal yang tak terelakkan dan dapat memicu konflik terbuka, maka perlu dilakukan *cyber diplomacy* untuk memitigasinya. Oleh karena itu, pertanyaan utama makalah ini adalah: Apa yang dimaksud dengan *cyber diplomacy* dan apa yang bisa dijanjikannya bagi penggunaan ruang siber yang damai?

KERANGKA TEORI

Untuk menjawab pertanyaan utama makalah ini, penulis menggunakan teori Diplomasi dari mazhab *English School*. Bagi mazhab *English School*, diplomasi merupakan inti dari politik internasional; diplomasi adalah lembaga sentral dalam definisi dan pemeliharaan masyarakat internasional (Hall, 2006; Neumann, 2002, 2003; Watson, 1982 dalam Barrinha & Renard, 2017, hal. 355). Alasan pemilihan teori Diplomasi karena teori ini dapat menjadi dasar bagi penjelasan mengenai diplomasi yang terjadi di ruang siber. Selain itu, keberadaan sesuatu yang asing, kondisi keberagaman, atau sesederhana keberadaan orang lain, dikombinasikan dengan kebutuhan untuk hidup berdampingan secara damai akan membutuhkan diplomasi (Hodzic, 2017, hal. 13).

Diplomasi adalah salah satu instrumen penting untuk mencapai kepentingan nasional negara dalam hubungan internasional. Dengan diplomasi, negara membangun citra dan gagasan tentang dirinya. Pada tahun 1959, Avalon Hill, sebuah perusahaan AS yang memproduksi *strategic board game*, merilis *Diplomacy*. Tujuan permainan ini adalah untuk mengendalikan titik pasokan di seluruh wilayah Eropa pra-Perang Dunia 1 melalui negosiasi, dengan "membentuk dan mengkhianati aliansi" dan menentukan "strategi yang menguntungkan", tanpa efek acak dari dadu. Representasi diplomasi sebagai tindakan penundukan negara yang rasional dan penuh perhitungan melalui negosiasi, menggambarkan beberapa aspek penting terhadap makna konsep (Parlett, 1999 dalam Hodzic, 2017, hal. 6).

Terdapat berbagai konsep diplomasi yang dikemukakan oleh para penulis. Bull (1977, hal. 156) memandang diplomasi sebagai suatu "perilaku hubungan antara negara dan entitas lain dalam politik dunia yang dilakukan oleh

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (311-333) doi: 10.24198/padjir.v1i3.26241

agen resmi dan dengan cara damai." Watson (1984, hal. 33) melihat diplomasi sebagai suatu proses "negosiasi antar entitas politik yang mengakui kemerdekaan satu sama lain." Definisi dari Bull dan Watson ini merupakan gagasan yang paling sering digunakan untuk mendefinisikan diplomasi. Kedua definisi ini memaparkan secara jelas fitur yang mendasar dari diplomasi, yaitu pendekatan tanpa penggunaan kekerasan untuk merekonsiliasi kepentingan-kepentingan di antara para aktor internasional, terutama negara. Bjola (2015) berpendapat bahwa meskipun dengan menggunakan cara-cara tanpa kekerasan, diplomasi di saat yang bersamaan membentuk konflik dan kerja sama dalam politik internasional.

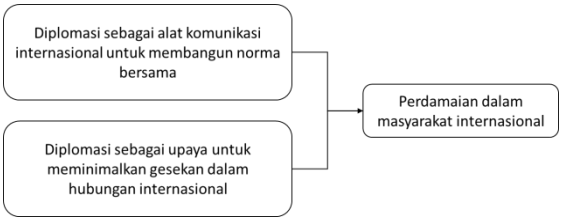
Diplomasi melibatkan jenis perilaku tertentu di antara para aktor internasional, tetapi menurut Bjola (2015) keberhasilan atau kegagalan suatu diplomasi sangat bergantung pada kemampuan para diplomat untuk secara tepat mengenali dinamika *power* yang berkembang. Hal yang menjadi aspek mendasar dari suatu hubungan diplomatik adalah mengelola perubahan. Pengamatan yang cermat dapat memunculkan poin-poin yang sangat penting jika berfungsinya masyarakat internasional adalah persoalan konstruksi yang berkelanjutan, legitimasi, adaptasi prinsip-prinsip bersama serta harapan intersubjektif dari perilaku internasional.

Selain itu, Wight (1979) berpendapat bahwa diplomasi, dipahami sebagai "upaya untuk menyesuaikan kepentingan yang saling bertentangan melalui negosiasi dan kompromi." Menurut Bull (2002), sebagaimana dikutip Barrinha dan Renard (2017), diplomasi merupakan "pemelihara gagasan masyarakat internasional, dengan kepentingan melestarikan dan memperkuatnya." Menurutnya, terdapat lima fungsi utama dalam praktik diplomasi: untuk memfasilitasi komunikasi dalam politik dunia, untuk menegosiasikan perjanjian, untuk mengumpulkan informasi dan intelijen dari negara lain, untuk menghindari atau meminimalkan "gesekan dalam hubungan internasional" (2002:165) dan, pada akhirnya, untuk melambangkan keberadaan masyarakat dalam negara.

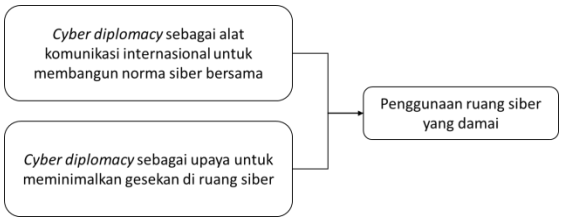
Saat ini, diplomasi tidak lagi hanya sekadar hubungan antar negara. Menurut Jonsson & Langhorne (2004), diplomasi harus mempertimbangkan "hubungan dan dialog yang lebih luas, yang melibatkan entitas seperti organisasi regional dan internasional–baik antarpemerintah (IGO) maupun non-pemerintah (LSM)–perusahaan multinasional, aktor sub-nasional, jaringan advokasi, dan individu-individu yang berpengaruh." (dalam Barrinha & Renard, 2017, hal. 355). Selain itu, dari tahun ke tahun diplomasi juga semakin meluas ke area-area kebijakan baru, memasuki wilayah politik yang belum terpetakan seperti negosiasi iklim atau masalah siber (Barrinha & Renard, 2017, hal. 355).

Dari berbagai definisi dan konsep yang dikemukakan oleh para penulis di atas, dapat penulis simpulkan bahwa untuk menciptakan perdamaian dalam masyarakat internasional, diplomasi harus berfungsi sebagai alat komunikasi internasional untuk membangun norma bersama dan sebagai cara untuk mengelola politik internasional yang bertujuan untuk meminimalkan gesekan dalam hubungan internasional. Jika dikaitkan dengan diplomasi dalam ruang siber, *cyber diplomacy* harus berfungsi sebagai alat komunikasi internasional untuk membangun norma siber bersama dan cara untuk mengelola ruang siber yang bertujuan untuk meminimalkan gesekan di ruang siber. Kedua fungsi inilah yang akan menjadi dasar analisis penulis dalam bab 2.

OPERASIONALISASI TEORI



MODEL ANALISIS



ARGUMENTASI UTAMA

Penulis berpendapat bahwa *cyber diplomacy* adalah praktik internasional yang muncul atas upaya membangun masyarakat siber internasional, dengan menjembatani antara kepentingan nasional negara dan dinamika masyarakat dunia. Oleh sebab itu, tujuan dari *cyber diplomacy* adalah untuk memenuhi fungsi-fungsi tradisional diplomasi, seperti menjaga perdamaian serta membangun rasa saling percaya di antara para pemangku kepentingan, dalam konteks siber. Melalui *cyber diplomacy*, pertentangan kepentingan negara-negara dapat dimitigasi agar tidak terjadi konflik terbuka sehingga terwujud ruang siber yang damai.

METODE RISET

Penulis menggunakan metode kualitatif dengan penulisan eksploratif analitis. Metode kualitatif digunakan karena dapat mencakup berbagai isu sosial dan mampu memberikan penjelasan, melakukan analisis, dan memberikan pemahaman terhadap berbagai fenomena sosial yang terjadi. Secara sederhana, John W. Creswell mendefinisikan penelitian kualitatif sebagai berikut:

> [a] *qualitative research begins with assumptions and the use of interpretive/theoretical frameworks that inform the study of research problems addressing the meaning individuals or groups ascribe to a social or human problem* (Cresswel, 2013, hal. 44).

Metode kualitatif menekankan pada kualitas analisis yang mengacu pada teori atau konsep. Penjabaran dalam metode kualitatif bersifat deskriptif atau penjelasan berupa kata dan bukan berupa angka. Menurut Djajasudarma (2009), metode penelitian kualitatif adalah metode yang bertujuan untuk memberikan deskripsi secara sistematis mengenai data, sifat-sifat, dan hubungan fenomena-fenomena yang akan diteliti. Ada dua alasan pemilihan metode kualitatif dalam makalah ini. Alasan pertama karena makalah ini adalah bagian dari kajian ilmu sosial dalam studi hubungan internasional seperti yang diutarakan oleh Creswell. Alasan kedua, dengan menggunakan metode kualitatif, akan diperoleh gambaran atau deskripsi yang jelas dan detail mengenai *cyber diplomacy*, segala dinamika yang terjadi di ruang siber, dan apa yang bisa dijanjikan *cyber diplomacy* bagi penggunaan ruang siber yang damai. Kemudian, metode pengumpulan data dilakukan dengan menganalisis dokumen seperti buku dan artikel dari jurnal-jurnal internasional, dan juga dari dari data *website* yang relevan.

PEMBAHASAN

Ruang Siber

Cyber diplomacy terjadi di ruang siber. Oleh karena itu, penting untuk memahami tentang ruang siber. Menurut Buck (1998), ruang siber memiliki karakteristik yang membingkai keterlibatan diplomatik di antara para pemangku kepentingan. Lebih lanjut ia menjelaskan bahwa ruang siber merupakan domain global yang menghubungkan berbagai negara dan masyarakat di seluruh dunia dalam berbagai cara, sehingga dapat terjadi interaksi dan juga gesekan di antara negara dan atau masyarakat. Menurutnya, ruang siber juga seringkali dianggap sebagai *global common*, atau domain sumber daya yang semua negara memiliki akses hukum terhadapnya (Buck, 1998, hal. 6). Ruang siber dapat dibandingkan dengan sumber daya global lainnya, seperti laut lepas, wilayah udara, dan luar angkasa. Dengan demikian, ruang siber membutuhkan serangkaian peraturan dan regulasi untuk memastikan akses bagi semua dan menghindari konflik. Hal ini dapat dicapai dengan negosiasi diplomatik. Karakteristik-

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (311-333) doi: 10.24198/padjir.v1i3.26241

karakteristik ruang siber menjadikan hubungan ruang siber internasional dan tata kelola ruang siber sangat kompleks dan rapuh, tetapi di saat yang bersamaan menjadikan diplomasi semakin diperlukan, terutama dalam mekanisme pembangunan kepercayaan serta pengembangan norma-norma dan nilai-nilai internasional.

Kemudian, perhatian terhadap isu-isu siber juga berubah. Barrinha & Renard (2017) menjelaskan bahwa isu siber mulanya dianggap sebagai masalah teknis semata, kemudian menjadi aspek eksternal dari kebijakan domestik, hingga akhirnya diakui sebagai topik utama dari kebijakan luar negeri. Lebih lanjut mereka mengatakan bahwa pada pergantian dekade pertama abad kedua puluh satu, beberapa negara dengan kekuatan siber besar mengeluarkan strategi keamanan siber pertama mereka, ketika ruang siber dan infrastruktur semakin dianggap sebagai aset strategis (Barrinha & Renard, 2017, hal. 358). AS merilis *Cyberspace policy review* pada tahun 2009, Inggris merilis *Cybersecurity Strategy* di tahun yang sama, sementara China menerbitkan *White Paper on the internet* pada tahun 2010 (Barrinha & Renard, 2017, hal. 358).

Berita tentang siber juga mengalami perubahan. Menurut Hodzic (2017), satu dekade yang lalu, berita tentang siber sebagian besar terkait dengan perkembangan teknologi internet dan kemajuan komunikasi. Saat ini, sebagian besar berita tentang siber terkait dengan kemampuan siber negara, keamanan, dan pertahanan (Hodzic, 2017, hal. 16). Selain menunjukkan semakin pentingnya siber dalam kehidupan sehari-hari dan politik, tren ini juga menggambarkan bahwa representasi umum siber adalah sebagian besar berbasis teknologi, yang menunjukkan adanya ruang artifisial bagi perpindahan kegiatan seperti komunikasi atau perang (Hodzic, 2017, hal. 16). Kemudian, tren ini juga mencerminkan pendekatan umum dalam mendefinisikan siber, yaitu "*Cyberspace* adalah dunia tanpa bentuk, nonfisik yang secara teoritis ada karena hubungan antara komputer, jaringan komputer, internet, dan perangkat serta komponen lain yang terlibat dalam penggunaan internet." (Lasky, 2017 dalam Hodzic, 2017, hal. 16).

Dalam Hubungan Internasional, saat ini ruang siber telah menjadi fokus yang signifikan. Topik ini menjadi arus utama karena sebagian besar aktor-aktor global telah menuangkan kebijakan-kebijakan luar negerinya dan mengadopsi berbagai langkah untuk mengejar tujuan-tujuan stategisnya di dalam ruang siber. Hal ini dapat dilihat misalnya pada penggunaan media sosial oleh Kementerian Luar Negeri untuk mempromosikan negara, kebijakan dan nilai-nilainya (Bjola & Pamment, 2019, hal. 1-2). Selain itu, ada juga kekhawatiran akan keamanan nasional di ruang siber, sehingga ruang siber menjadi ruang politik yang diperebutkan, dibentuk oleh kepentingan, norma, dan nilai yang berbeda. Politisasi ruang siber ini membuat para diplomat memiliki peran penting dalam menganalisis dan menengahi masalah-masalah yang muncul.

Diplomasi Siber

Seiring dengan perkembangan internet, *cyber diplomacy* juga semakin sering dilakukan. Hodzic (2017) menyebutkan bahwa istilah *cyber dyplomacy* atau diplomasi dunia maya semakin banyak digunakan oleh para aktor utama dalam politik global untuk menggambarkan transformasi dalam pelaksanaan diplomasi di era digital. Menurutnya, evolusi diplomasi di ruang siber berkisar pada pemanfaatan media sosial baru, orientasi terhadap aktor publik, dan penetapan ancaman siber dan perilaku siber sebagai area baru dalam politik internasional (Hodzic, 2017, hal. 1). Selain itu, *cyber diplomacy* juga dapat dikatakan sebagai evolusi dari diplomasi publik dan sering kali disebut sebagai diplomasi publik 2.0. Perkembangan *cyber diplomacy* merupakan respons terhadap pergeseran dalam hubungan internasional.

Terdapat banyak definisi *dari cyber diplomacy*. Pertama, c*yber diplomacy* dapat

didefinisikan sebagai upaya untuk memfasilitasi komunikasi, menegosiasikan perjanjian, mengumpulkan informasi dan intelijen dari negara lain untuk menghindari gesekan di ruang siber, dengan mengacu pada agenda kebijakan luar negeri. Kedua, c*yber diplomacy* dilihat sebagai upaya untuk menggunakan sumber daya dan fungsi diplomatik untuk mengamankan kepentingan nasional terkait ruang siber. Secara umum, strategi ruang siber nasional atau *cybersecurity* menawarkan gagasan mengenai agenda luar negeri yang mencakup keamanan siber, kejahatan dunia maya, pembangunan kepercayaan, kebebasan internasional, dan tata kelola internet. Ketiga, *cyber diplomacy* juga dapat diartikan sebagai diplomasi di dalam domain siber atau penggunaan sumber daya diplomatik dan kinerja fungsi diplomatik untuk mengamankan kepentingan negara terkait ruang siber. Kepentingan-kepentingan tersebut pada umumnya diidentifikasi dalam strategi ruang siber (*cyberspace*) suatu negara atau keamanan siber (*cybersecurity*), yang disertakan ke dalam agenda-agenda diplomatik. *Cyber diplomacy* dalam praktiknya melibatkan diplomasi, resolusi konflik, perjanjian dan kebijakan yang mengelilingi dunia siber.

Begitu juga dengan isu dalam *cyber diplomacy*, ada banyak isu yang dibahas di dalamnya. Barrinha dan Renard (2017) mencatat isu-isu dominan dalam agenda *cyber dyplomacy* diantaranya keamanan siber (*cyber security*), kejahatan siber (*cybercrime*), pembangunan kepercayaan (*confidence-building*), kebebasan internet (*internet freedom*), dan tata kelola internet (*internet governance*). Oleh karena itu, menurut mereka, *cyber diplomacy* dilakukan sebagian atau sepenuhnya oleh diplomat, yang bertemu dalam format bilateral (seperti dialog AS-China) atau dalam forum multilateral (seperti di PBB). Selain diplomasi tradisional, diplomat juga berinteraksi dengan berbagai aktor non-negara, seperti pemimpin perusahaan internet (misalnya Facebook atau Google), pengusaha teknologi atau organisasi masyarakat sipil (Barrinha & Renard, 2017, hal. 355). Diplomasi juga dapat melibatkan pemberdayaan suara-suara yang tertindas di negara-negara lain melalui teknologi (Owen, 2015 dalam Barrinha & Renard, 2017, hal. 355).

Cyber diplomacy dapat dilakukan oleh negara dan aktor non-negara. *Cyber diplomacy* yang dilakukan oleh negara terdapat di dua level, yaitu Kementerian Luar Negeri dan kedutaan yang berlokasi di seluruh dunia (Manor & Segev, 2015, hal. 94). Menurut Manov dan Segev, dengan beroperasi pada dua level ini, negara-negara dapat menyesuaikan pesan kebijakan luar negeri dan citra negaranya sesuai dengan karakteristik dari khalayak lokal–misalnya sejarah, budaya, nilai-nilai, dan tradisi mereka– agar dapat mencapai target kebijakan luar negeri dan citra yang ingin mereka bangun (2015, hal. 94).

Kebijakan yang diambil oleh negara-negara terkait dengan ruang siber membuat *cyber diplomacy* berkembang. Barrinha dan Renard (2017) menyebutkan bahwa titik awal dari *cyber diplomacy* dapat ditemukan dalam publikasi strategi internasional AS untuk ruang siber pada tahun 2011. Menurut mereka, publikasi ini merupakan dokumen pemerintah pertama di dunia yang berfokus sepenuhnya pada aspek internasional dari isu-isu siber, dan di dalamnya diidentifikasi sejumlah prioritas, yaitu ekonomi, perlindungan jaringan, penegakan hukum, militer, tata kelola internet, pembangunan internasional dan kebebasan internet; serta mengandalkan tiga pilar untuk mencapai prioritas-prioritas tersebut, yaitu diplomasi, pertahanan, dan pembangunan (3D) (Barrinha & Renard, 2017, hal. 359). Sejalan dengan strategi ini, *Office of the Coordinator for Cyber Issues* didirikan dalam Departemen Luar Negeri AS, yang menjadi badan pertama yang sepenuhnya didedikasikan untuk isu-isu siber pada kedutaan luar negeri di seluruh dunia, dan Koordinator Christopher Painter menjadi *cyber diplomat* pertama di dunia (Barrinha & Renard, 2017, hal. 359).

Setelah AS mempublikasikan strategi ruang sibernya, negara-negara lain juga merumuskan

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (311-333) doi: 10.24198/padjir.v1i3.26241

strateginya masing-masing. Namun, menurut Barrinha & Renard, meski saat ini semakin banyak negara yang mengadopsi strategi keamanan siber untuk mengatasi konsekuensi internasional dari isu-isu siber, hanya sedikit negara yang mengadopsi strategi internasional yang berdiri sendiri seperti yang dilakukan AS, diantaranya adalah Strategi Internasional Jepang tentang Kerjasama Keamanan Siber yang diadopsi pada tahun 2013, Kesimpulan Dewan tentang Diplomasi Siber yang diadopsi oleh negara-negara anggota Uni Eropa pada tahun 2015 – di sini pertama kalinya istilah "*cyber diplomacy*" digunakan dalam dokumen resmi pemerintah–dan Strategi Keamanan Siber Australia pada tahun 2016 yang berkomitmen untuk membangun Strategi Keterlibatan Internasional (Barrinha & Renard, 2017, hal. 359).

Pengaruh perkembangan siber terhadap diplomasi dapat dilihat dari dua sisi. Menurut Hodzic (2017), ketika diamati sebagai tindakan pelaksanaan kebijakan luar negeri negara oleh perwakilan resmi, siber mengubah diplomasi dalam dua cara, yaitu dengan menstimulasi pergeseran dalam distribusi kekuasaan dan memunculkan metode-metode baru dalam pelaksanaan tugas-tugas diplomatik. Ia menjelaskan bahwa, saat negara memperoleh keunggulan komparatif dengan teknologi siber, posisinya dalam sistem juga berpotensi untuk berubah (Hodzic, 2017, hal. 26). Terkait dengan metode, serangan siber tidak membutuhkan sumber daya yang sama seperti yang dibutuhkan oleh *hard power*, demikian pula representasi siber tidak membutuhkan sumber daya yang berada di kedutaan besar di luar negeri (Hodzic, 2017, hal. 26). Ia juga menambahkan bahwa saat ini dominasi negara dalam penetapan kebijakan luar negeri ditantang oleh keberadaan aktor transnasional, perusahaan swasta, dan publik yang keberadaannya semakin diperhitungkan yang secara internal menuntut negara agar lebih bertanggung jawab, dan secara eksternal merespons penyebab-penyebab global yang melampaui kepentingan satu negara (Hodzic, 2017, hal. 26-27). Sementara itu, ketika dilihat sebagai pengelolaan friksi kepentingan negara, diplomasi dalam siber tidak hanya mengelola ranah lokal, nasional, non-teritorial, dan global dalam "montase arus virtual dan ruang siber" (Deibert, 2002 dalam Hodzic, 2017, hal. 27) atau mengelola kemampuan siber yang semakin meningkat dalam menetapkan agenda, tetapi *cyber diplomacy* harus mengelola kompleksitas dan ambiguitas yang timbul dari pergeseran kekuatan baru dan memiliki kapasitas untuk melakukan *reframing* (Hodzic, 2017, hal. 27).

Meski mengalami peningkatan, *cyber diplomacy* yang dilakukan oleh negara-negara jarang terdengar. Menurut Barrinha & Renard (2017), peran diplomasi di ruang siber tidak menonjol di media jika dibandingkan dengan cerita tentang insiden siber seperti spionase siber, serangan siber, kegiatan peretasan, sensor internet, dan masalah teknis lainnya yang disebut sebagai masalah keamanan nasional, atau muncul dalam berita ketegangan diplomatik antarnegara. Pengecualiannya adalah kesepakatan keamanan siber pada tahun 2015 yang dicapai oleh AS dan China, yang merupakan salah satu masalah paling kontroversial dalam hubungan bilateral keduanya (Barrinha & Renard, 2017, hal. 353). Selama bertahun-tahun, kedua belah pihak saling menuduh adanya infiltrasi jaringan dan pencurian informasi rahasia dari perusahaan dan lembaga pemerintah (Barrinha & Renard, 2017, hal. 353).

Penggunaan Diplomasi Siber

Penggunaan *cyber diplomacy* dapat dilihat dari beberapa perspektif, yaitu diplomat, negara, dan aktor non-negara. Menurut Sotiriu, dari perspektif praktisi seperti diplomat, penggunaan *cyber diplomacy* dapat meningkatkan audiensi dari pesan mereka, menghubungkan mereka langsung dengan masyarakat, tanpa melalui media yang dikendalikan oleh pemerintah dan negara yang berpotensi mengubah pesan awal (Sotiriu, 2015, hal. 41). Bjola dan Jiang (2015, hal. 87)

menambahkan bahwa jika dibandingkan dengan sarana komunikasi yang lebih konvensional, media sosial menghadirkan tiga keuntungan utama dalam melakukan diplomasi publik, yaitu (1) menawarkan instrumen yang sangat efektif untuk menyampaikan informasi; (2) memungkinkan pesan yang dimaksudkan untuk menjangkau lebih jauh ke target audiens; dan (3) memungkinkan komunikasi dua arah antara diplomat dan publik asing. Namun, menurut mereka, perspektif holistis yang menggabungkan media sosial dengan bentuk interaksi diplomatik yang lebih tradisional cenderung memberikan hasil yang lebih baik (Bjola & Jiang, 2015, hal. 87). Media sosial dapat membantu menyampaikan pesan yang kuat dengan cara yang sangat efektif, tetapi tidak dapat bertindak sebagai pengganti dari perencanaan strategi yang baik, pengelolaan hubungan dan krisis, yang merupakan ciri dari perilaku diplomatik profesional (Bjola & Jiang, 2015, hal. 87).

Dari perspektif negara, *cyber diplomacy* dapat menjadi sarana komunikasi untuk menciptakan perdamaian antarnegara. Contohnya dapat dilihat dari upaya Israel untuk membuka sebuah kedutaan virtual bagi negara-negara Teluk Persia (juga dikenal sebagai *Gulf Cooperation Council* atau GCC) pada tahun 2013, terpisah dari negosiasi komunikasi, perdagangan, dan kerja sama yang sudah ada sebelumnya tetapi dilakukan secara tertutup (Sotiriu, 2015, hal. 45). Sebelum Israel, Amerika Serikat (AS) lah yang pertama kali membuka kedutaan virtual "di" Iran pada tahun 2011 untuk meningkatkan peluang dialog dengan rakyat Iran, dan bagi AS untuk mempromosikan kebijakan, budaya, dan rakyat Amerika, serta membawa informasi dan sudut pandang alternatif bagi rakyat Iran yang berbeda dari sumber-sumber resmi pemerintah (Sotiriu, 2015, hal. 45). Namun, terlepas dari janji bahwa kehadiran kedutaan virtual ini diadakan untuk rakyat Iran, dalam dua belas jam pertama sejak diluncurkan, kedutaan ini ditutup oleh pemerintah Iran (dalam arti rakyat Iran dicegah mengaksesnya), meskipun situs web ini secara teratur diperbarui, bahkan terdapat salam dari Presiden Obama untuk Nowruz 2014 (Sotiriu, 2015, hal. 46). Di sini terlihat bahwa upaya diplomasi suatu negara belum tentu dapat diterima dengan baik oleh negara lainnya.

Upaya lainnya dari negara untuk menciptakan perdamaian melalui *cyber diplomacy* juga diteliti oleh Bjola dan Jiang. Menurut mereka, para diplomat dari Uni Eropa (UE), Jepang, dan AS di kantor kedutaan mereka di Beijing secara kreatif menggunakan media sosial, situs *microblogging* China Weibo, untuk mengurangi kecurigaan pemerintah China, dan dengan demikian berhasil membangun saluran komunikasi yang terbuka dengan rakyat China (Bjola, 2015, hal. 6). Mereka berkesimpulan bahwa *cyber diplomacy* digunakan terutama sebagai instrumen penyebaran informasi. Hal ini misalnya dilakukan oleh UE yang mempromosikan budaya Eropa kepada warga China untuk meningkatkan visibilitas UE di antara warga China, yang bisa dibilang belum memiliki pemahaman yang jelas tentang kawasan tersebut (Bjola & Jiang, 2015, hal. 86).

Saat ini, upaya pembentukan citra negara di dunia internasional juga dilakukan melalui *cyber diplomacy*. Pemerintah dan pejabat di berbagai negara menggunakan situs jejaring sosial seperti Facebook dan Twitter sebagai bagian dari praktik sehari-hari mereka. Saluran *cyber diplomacy* yang dioperasikan oleh Kementerian Luar Negeri khususnya menarik khalayak yang luas dan beragam, mulai dari individu, wartawan, pembuat kebijakan, hingga kementerian dan kedutaan asing lainnya. Dengan demikian, akun media sosial resmi semakin banyak digunakan sebagai alat untuk menyajikan dan membentuk citra negara (*nation-branding*) di seluruh dunia (Bjola, 2015, hal. 7). Manor dan Segev mencontohkan tindakan *nation-branding* yang dilakukan oleh AS setelah peristiwa 9/11. Amerika melambangkan nilai-nilai seperti demokrasi, kebebasan, kemakmuran, dan hak asasi manusia, tetapi serangan teroris 9/11 dan respons AS terhadap serangan ini mengubah

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (311-333) doi: 10.24198/padjir.v1i3.26241

pandangan khalayak terhadap AS dan mengubah nilai-nilai yang dianggap sebagai "Amerika" (Manor & Segev, 2015, hal. 95). Perang global melawan teror dan invasi militer ke Irak dan Afghanistan membuat banyak orang memandang AS arogan, imperialistik, dan merupakan ancaman bagi perdamaian dunia (Silver & Hill, 2002; Rawson, 2007; Quelch & Jocz, 2009 dalam Manor & Segev, 2015, hal. 95). Manor dan Segev berpendapat bahwa persepsi baru tentang AS, dan transisinya dari suar demokrasi ke kerajaan militeristik, menyebabkan krisis citra "Amerika" (2015, hal. 95). Lebih lanjut mereka menyebutkan bahwa pembentukan citra melalui *cyber diplomacy* merupakan cara yang ampuh yang memungkinkan AS mengubah citra dan reputasi globalnya, dan kemudian merevitalisasi citra "Amerika" (2015, hal. 96).

Namun, Manor dan Segev mengingatkan bahwa penilaian hasil dari tindakan pembentukan citra negara penting untuk dilakukan. Analisis ini menurut mereka dapat dilakukan oleh direktur media sosial baik di tingkat kedutaan maupun kementerian untuk mengukur keefektifan dari pesan yang disampaikan dan bagaimana pesan disebarkan (2015, hal. 107). Mereka mengilustrasikannya dengan *tweet* yang dibuat oleh mantan Ibu Negara AS, Michele Obama, pada 8 Mei 2014. Ia mengunggah *selfie* dengan tagar *#Bringbackourgirls*, yang merujuk pada lebih dari 200 gadis yang diculik oleh kelompok Islamis di Nigeria. Tanggapan terhadap *tweet* ini, yang muncul di akun media sosial Departemen Luar Negeri AS, adalah banyaknya orang yang mengunggah foto *selfie* dengan tagar *#Bringbackyourdrones*, yang merujuk pada seringnya penggunaan *drone* oleh militer AS untuk membunuh tersangka teroris (2015, hal. 107). Ini menunjukkan bahwa reaksi khalayak tidak sesuai dengan tujuan dari pesan yang dibuat.

Selain itu, *cyber diplomacy* juga dapat digunakan oleh aktor non-negara untuk mengkampanyekan perdamaian atau melawan musuh bersama seperti teroris. Hal ini dapat dilihat dalam protes berskala besar yang diorganisasi melalui Facebook, Skype dan pesan instan melawan Angkatan Bersenjata Revolusioner di Columbia (FARC) di hampir 200 kota di seluruh dunia, yang akhirnya menjadi protes terbesar terhadap organisasi teroris dalam sejarah (Lichtenstein, 2010 dalam Sotiriu, 2015, hal. 44). Kemudian, ada juga kampanye Facebook *Israel Loves Iran*, yang berupaya untuk menyatukan rakyat Israel dan Iran serta untuk mempromosikan perdamaian di antara kedua negara. Sejak dimulai pada tahun 2012, gerakan media sosial ini sekarang pengikutnya di Facebook berjumlah lebih dari 120 ribu orang yang berasal dari seluruh dunia dan memicu kampanye lainnya yang berfokus pada perdamaian di Timur Tengah (Sotiriu, 2015, hal. 44).

Ancaman di Ruang Diber

Kemajuan internet telah membawa perubahan yang besar dalam kehidupan kita saat ini. Semua kalangan, mulai dari negara, bisnis, hingga individu semakin bergantung pada internet untuk melakukan aktivitas sehari-harinya. Ketergantungan ini menurut Roche dapat menimbulkan ancaman terhadap infrastruktur, proses politik, dan privasi individu (2019, hal. 68).

Ancaman dalam Infrastruktur Ruang Siber

Serangan siber yang dilakukan baik oleh negara maupun aktor non-negara semakin meningkat jumlahnya. Putra dan Punzalan menyebutkan bahwa China, sebagai negara asal, menyumbang 22 persen dari total serangan yang dilakukan terhadap pemerintah di seluruh dunia (2013, hal. 269). Menurut mereka, bentuk serangan yang paling umum terhadap sektor pemerintah adalah *Denial of Service attack* (DDoS). DDoS adalah kondisi ketika komputer *host* (atau server web), yang menampung situs web yang ditargetkan, tidak dapat menanggapi atau berkomunikasi dengan

komputer lainnya karena sumber dayanya telah digunakan oleh rentetan permintaan dari para penyerang (Putra & Punzalan, 2013, hal. 270). Putra dan Punzalan menambahkan bahwa 28 persen serangan berasal dari AS dan menargetkan sektor pemerintah di Eropa, Timur Tengah, dan Afrika. Dalam beberapa tahun terakhir dan mungkin karena resesi ekonomi global, peretasan telah berubah dari hobi pribadi menjadi aktivitas bisnis kriminal yang terorganisir (Putra & Punzalan, 2013, hal. 269). Selain proliferasi kejahatan siber dan spionase siber, peningkatan juga terjadi pada jumlah insiden perang siber internasional dan terorisme siber (2013, hal. 269).

Dari tahun 2005 hingga 2009, serangan siber terjadi di beberapa negara. Putra dan Punzalan (2013) memberikan contoh beberapa negara yang menerima serangan. Menurut sebuah laporan dari Pusat Keamanan dan Diplomasi Maritim Malaysia, beberapa situs web pemerintah, universitas dan institusi swasta Malaysia diduga ditembus oleh peretas Indonesia ketika terjadi perselisihan Ambalat antara Malaysia dan Indonesia pada tahun 2005. Laporan tersebut juga menyebutkan bahwa peretas meninggalkan pesan berikut di situs web Departemen Pekerjaan Umum:

> *With respect,*
>
> *In the name of the law, I order you, Malaysian government, please retreat from Indonesian area. Please don't be too greedy. Indonesia is having bad days recently. The natural disasters, increasing poverty, etc. Your country is much more prosperous than Indonesia. Don't you be ashamed?*
>
> *FYI. I'm not a hacker.*

Selanjutnya, Georgia, yang merupakan bekas negara Soviet, mengalami "pengepungan siber" pada Agustus 2008 (Putra & Punzalan, 2013, hal. 270). Serangan DDoS dilakukan terhadap beberapa situs web pemerintah setelah periode konflik bersenjata antara Georgia dan Rusia karena masalah Ossetia Selatan (Putra & Punzalan, 2013, hal. 271). Pada Juli 2009, Korea Selatan dan AS menjadi sasaran tiga gelombang serangan DDoS. Menurut laporan berita, sebuah surat kabar nasional terkemuka dan agen mata-mata Korea Selatan dihantam oleh tingginya volume lalu lintas internet yang tidak wajar. Di AS, Gedung Putih dan Pentagon menjadi sasaran (Putra & Punzalan, 2013, hal. 271).

Ancaman terhadap Proses Politik

Ancaman terhadap proses politik dapat terjadi kertika informasi yang beredar secara *online* dibuat untuk menguntungkan pihak tertentu atau menyudutkan lawan politik. Ancaman ini dapat muncul baik dari dalam negara maupun dari negara lainnya. Intervensi dalam pemilihan umum AS pada tahun 2016 merupakan contoh bagaimana teknologi digunakan oleh pihak asing untuk ikut campur dalam urusan internal saingannya (Roche, 2019, hal. 69).

Contoh lainnya adalah perang informasi. Chansoria (2012) berpendapat bahwa perang informasi, khususnya digital, telah membuat ruang siber menjadi sebuah ranah untuk melanggar perbatasan, menantang batas negara, dan yang paling penting, memungkinkan militer suatu negara untuk mencapai tujuan politik tertentu, dengan bentuk propaganda yang lebih tepat. Ia juga menyatakan bahwa potensi konflik di masa depan dalam abad ke-21 tidak akan hanya terbatas pada lingkup militer tradisional, dan meningkatnya ketergantungan pada ruang siber membuat isu-isu yang berkaitan dengan keamanan nasional semakin rentan (Chansoria, 2012, hal. 106). Menurutnya hal ini dikarenakan taktik perang siber relatif berbiaya rendah dan selalu tersedia, sehingga menjadikannya lebih menarik bagi negara maupun aktor non-negara untuk mengeksploitasi keterampilan peretas atau yang disebut 'pejuang siber patriotik' (Chansoria, 2012, hal. 106).

Dampak dari perang informasi sangat besar. Perang informasi mengaburkan batas antara otonomi militer dan sosial, serta antara

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (311-333) doi: 10.24198/padjir.v1i3.26241

perdamaian dan perang, sehingga memungkinkan disrupsi sosial yang tak terbayangkan (Chansoria, 2012, hal. 106). Mengutip Dibb (1997-1998), Chansoria menyatakan bahwa konflik antarnegara akan berubah menjadi kapasitas untuk menyerang dan melumpuhkan transportasi, pasokan energi, dan jaringan komunikasi musuh dengan menggunakan teknologi komputer (2012, hal. 106). Ia menyimpulkan bahwa arus informasi global adalah salah satu dari banyak isu keamanan sumber daya dan non-militer yang memengaruhi politik domestik dan internasional, mengabaikan batas-batas politik atau geografis, dan semakin berada di luar prerogatif kekuasaan negara (Chansoria, 2012, hal. 106-107).

Ancaman terhadap Privasi

Informasi pribadi yang kita simpan secara *online* membuat kita rentan akan kehilangan privasi karena informasi tersebut dapat dengan mudah diakses oleh pihak-pihak yang mempunyai kepentingan tertentu. Jumlah data tentang informasi pribadi yang tersedia bagi pemerintah, perusahaan *marketing*, penyelidik, bahkan penjahat luar bisa besarnya (Roche, 2019, hal. 70). Tindakan pelanggaran terhadap privasi seperti pencegatan pesan internet, pemblokiran konten, perekaman pembicaraan di telepon, pelacakan lokasi keberadaan juga marak terjadi. Di AS, pemantauan pemerintah atas komunikasi dan data pribadi dimungkinkan oleh *Patriot Act* (Roche, 2019, hal. 70). Perusahaan swasta juga mengeksploitasi data pribadi yang sangat besar jumlahnya untuk dijual (Roche, 2019, hal. 70).

Cyber Diplomacy bagi Penggunaan Ruang Siber yang Damai

Bagaimana *cyber diplomacy* digunakan untuk mengatasi ancaman di ruang siber dan mewujudkan penggunaan ruang siber yang damai bisa kita lihat dari dua fungsi utamanya, yaitu sebagai alat komunikasi untuk membangun norma bersama dan sebagai upaya untuk meminimalkan gesekan di ruang siber.

Cyber Diplomacy sebagai Alat Komunikasi Internasional untuk Membangun Norma Siber Bersama

Untuk mewujudkan penggunaan ruang siber yang damai, *cyber diplomacy* dapat dijadikan sebagai alat komunikasi bagi negara-negara untuk membangun norma-norma internasional. Menurut Roche, teori di balik pembangunan norma-norma ini adalah jika sering dipraktikkan, seiring dengan waktu suatu sistem hukum internasional yang mengikat akan berkembang (2019, hal. 71). Norma-norma ini menuntut negara untuk saling bekerja sama, sehingga dapat menciptakan stabilitas di ruang siber (Roche, 2019, hal. 71). Upaya untuk membangun norma siber bersama telah digagas oleh berbagai negara, organisasi internasional, dan perusahaan teknologi swasta, diantaranya adalah *NATO Talinn Manual*, *Microsoft Norms Paper*, *Code of* Conduct–yang digagas oleh China, Rusia dan negara lainnya–*US Government Policy*, dan *United Nations Group of Governmental Expert on Information Security* (UN GGE) (Wibisono, 2018, hal. 5).

NATO Talinn Manual on the International Law Applicable to Cyber Warfare dikeluarkan oleh *Cooperative Cyber Defense Center of Excellence* (CCD COE) pada tahun 2013. Gagasan utama dalam manual ini adalah prinsip dasar dalam memastikan keamanan dan stabilitas ruang siber global (Wibisono, 2018, hal. 5). Kemudian, CCD COE mengeluarkan versi keduanya pada tahun 2017, yaitu *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, dengan memperluas cakupan dari hukum internasional yang mengatur perang siber ke rezim hukum di masa damai (Schmitt, 2017) dan membahas insiden yang sering dan umum terjadi (CCD COEa, t.t.). *Tallinn Manual 2.0* ini juga membahas topik-topik seperti kedaulatan, tanggung jawab negara, hak asasi manusia, serta hukum udara, ruang

angkasa, dan laut (Schmitt, 2017). Analisis *Tallinn Manual 2.0* bertumpu pada pemahaman bahwa hukum internasional era pra-siber berlaku untuk operasi siber, baik yang dilakukan oleh negara maupun yang ditujukan kepada negara. Ini berarti bahwa peristiwa siber tidak terjadi dalam kehampaan hukum dan negara memiliki hak dan kewajiban menurut hukum internasional (CCD COEb, t.t.).

Fokus dari *Tallinn Manual 1.0* adalah pada operasi siber yang paling berat, yang melanggar larangan penggunaan kekuatan dalam hubungan internasional, memberikan hak kepada negara-negara untuk menggunakan hak bela diri, dan/atau yang terjadi selama konflik bersenjata. Kemudian, *Tallinn Manual 2.0* menambahkan analisis hukum tentang insiden siber yang lebih umum yang dihadapi negara setiap harinya dan berada di bawah ambang batas penggunaan kekerasan atau konflik bersenjata (CCD COEb, t.t.). Pada dasarnya, menurut CCD COE, kedua manual ini bertujuan untuk menawarkan panduan dalam menerapkan norma-norma internasional yang ada ke ruang siber, yang terdiri dari aturan-aturan '*black letter*' dan didasarkan pada konsensus dari sekelompok ahli hukum internasional. Selain itu, kedua manual ini dirancang untuk memberikan panduan bagi penasihat hukum pemerintah dan mendorong penelitian lebih lanjut (CCD COEa, t.t.).

Selanjutnya, ada *Microsoft Norms Paper* yang digagas oleh Microsoft, sebuah perusahaan teknologi AS, pada Desember 2014. Wibisono menyebutkan bahwa *paper* ini merupakan norma-norma keamanan siber internasional yang bertujuan untuk mengurangi konflik di dunia yang tergantung pada internet dan gagasan utamanya adalah pada tanggung jawab negara untuk menghindari dan mencegah jenis serangan siber tertentu diluncurkan dari wilayahnya (2018, hal. 5).

Gagasan ketiga adalah *International Code of Conduct for Information Security*. *Code of conduct* ini digagas oleh negara-negara anggota *Shanghai Cooperation Organization* (SCO) yang terdiri dari China, Rusia, Kazakhstan, Kirgistan, Tajikistan, dan Uzbekistan (McKune, 2015). SCO kemudian mengajukan *code of conduct* ini kepada Majelis Umum PBB untuk dipertimbangkan pada Januari 2015 (McKune, 2015). Gagasan utama dari *code of conduct* ini adalah pada tanggung jawab negara untuk meningkatkan keamanan informasi dan sistem di dalam wilayah mereka (Wibisono, 2018, hal. 5). Menurut SCO, *code of conduct* ini dimaksudkan "untuk mendorong debat tentang norma-norma internasional dari keamanan informasi, dan membantu membentuk konsensus awal tentang isu ini" (dalam McKune, 2015). Namun, menurut McKune, dokumen ini masih menimbulkan keprihatinan serius mengenai hak asasi manusia. Lebih lanjut ia menjelaskan bahwa narasi dari *code of conduct* ini menekankan pada kedaulatan negara dan teritorial dalam ruang digital di atas segalanya, serta didominasi oleh intelijen, keamanan nasional, dan imperatif stabilitas rezim. Selain itu, mungkin yang paling mengkhawatirkan, tren yang diwujudkan oleh SCO dan tercermin dalam *code of conduct* itu sendiri adalah pada saran revisionisme strategis oleh negara-negara anggota SCO untuk hukum hak asasi manusia internasional (McKune, 2015).

Di tahun yang sama dengan *code of conduct* yang dimotori oleh CSO, AS mengeluarkan kebijakan tentang ruang sibernya. Kebijakan ini disampaikan oleh Menteri Luar Negeri AS John Kerry dalam sambutannya di Korea University, Seoul pada Mei 2015, ketika ia berbicara mengenai internet yang terbuka dan aman (U.S. Department of State, 2015). Tema utama dari kebijakan ini adalah pada tugas negara untuk saling bekerja sama dalam memitigasi jenis insiden siber tertentu (Wibisono, 2018, hal. 5). Hal ini tergambarkan dalam pernyataan yang disampaikan oleh Menteri Luar Negeri AS John Kerry sebagai berikut:

> *America's policy is to promote international cyber stability. The goal is to create a climate in which all states are*

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (311-333) doi: 10.24198/padjir.v1i3.26241

> *able to enjoy the benefits of cyberspace; all have incentives to cooperate and avoid conflict; and all have good reason not to disrupt or attack one another. To achieve this, we are seeking a broad consensus on where to draw the line between responsible and irresponsible behaviour* (U.S. Department of State, 2015).

Ketidaksepakatan dengan apa yang diajukan oleh negara-negara anggota SCO juga tergambarkan dalam pernyataan John Kerry berikut ini:

> *This is truly a point of separation in our era – now, in the 21st century. It's a point of separation between governments that want the internet to serve their citizens and those who seek to use or restrict access to the internet in order to control their citizens. …… there are more than a few who want to harvest the economic benefits of the internet while nevertheless closing off the avenues of political, social, and religious expression. They impose filters that eliminate broad categories of what their citizens can see and receive and transmit – and with whom ideas may be changed and shared. What's more, the governments that have pioneered the repressive use of such technologies are quick to export their tools and methods to others, and thereby further diminish individual rights* (U.S. Department of State, 2015).

Gagasan norma siber internasional kelima dikemukakan oleh *United Nations Group of Governmental Expert on Information Security* (UN GGE). UN GGE merupakan kumpulan para ahli yang berasal dari 20 negara dan gagasan utama mereka adalah pembatasan dalam pengembangan atau penggunaan senjata siber di masa damai (Wibisono, 2018, hal. 5). Ke-20 negara yang tergabung dalam UN GGE adalah Belarus, Brasil, China, Kolombia, Mesir, Estonia, Prancis, Jerman, Ghana, Israel, Jepang, Kenya, Malaysia, Meksiko, Pakistan, Korea Selatan, Rusia, Spanyol, Inggris, Irlandia Utara, dan AS (Wibisono, 2018, hal. 5). Wibisono mencatat bahwa pada pada Juli 2014 hingga Juni 2015, UN GGE membahas mengenai ancaman siber yang ada dan mulai muncul; norma, aturan dan prinsip untuk perilaku negara yang bertanggung jawab; *confidence building measures* (CBMs); Kerjasama internasional dan bantuan dalam keamanan dan pengembangan kapasitas ICT; dan bagaimana hukum internasional berlaku untuk penggunaan ICT (2018, hal. 6). Hasil dari pembahasan tersebut adalah 11 norma, aturan, atau prinsip yang bersifat sukarela dan tidak mengikat bagi perilaku negara yang bertanggung jawab, yang bertujuan mempromosikan lingkungan ICT yang terbuka, aman, stabil, mudah diakses, dan damai. Ke-11 norma, aturan, atau prinsip tersebut adalah (1) Menjaga perdamaian & keamanan internasional; (2) Mempertimbangkan konteks peristiwa, tantangan dan konsekuensi yang lebih besar dari insiden ICT; (3) Tidak digunakan untuk tindakan yang salah secara internasional; (4) Tindakan kooperatif untuk mengatasi ancaman; (5) Resolusi HRC 20/8 dan 26/13, resolusi GA 68/167 dan 69/166; (6) Tidak bertentangan dengan kewajiban ICT untuk infrastruktur penting; (7) Mengambil tindakan yang tepat untuk melindungi infrastruktur penting – resolusi GA 58/199; (8) Menanggapi permintaan bantuan yang sesuai dari negara lain; (9) Mengambil langkah-langkah yang tepat untuk memastikan integritas *supply chain*; (10) Pelaporan yang bertanggung jawab atas kerentanan ICT dan solusi yang tersedia; dan (11) Tidak merusak sistem informasi dari tim tanggap darurat resmi/tidak menggunakannya untuk terlibat dalam kegiatan kejahatan internasional (Wibisono, 2018, hal. 7). Meskipun UN GGE dianggap berhasil, Wibisono menyebutkan bahwa UN GGE gagal menyepakati sidang berikutnya pada tahun 2017 (2018, hal. 7). Namun, pada Desember 2018, Majelis Umum PBB membentuk GGE yang baru dan *Open-Ended Working Group* (OEWG) guna melanjutkan sidang untuk periode 2019-2020 dan 2020-2021.

Dari kelima gagasan norma internasional bersama tersebut, Wibisono membuat beberapa kesimpulan. Pertama, konvergensi dari gagasan-gagasan tersebut bersifat superfisial, karena hanya berisikan prinsip-prinsip umum dan upaya saling membantu. Kedua pertentangan dalam hal batas kedaulatan negara tetap ada karena faktor budaya, politik, dan militer. Ketiga, distribusi kemampuan siber yang asimetris memengaruhi preferensi dan penekanan pada norma (2018, hal. 5).

Cyber Diplomacy sebagai Upaya untuk Meminimalkan Friksi di Ruang Siber

Selain pembangunan norma, *cyber diplomacy* juga merupakan upaya untuk meminimalkan gesekan di ruang siber. Upaya yang dapat dilakukan adalah dengan mengembangkan kebijakan ruang siber internasional. Menurut Wibisono, jika dilihat dari dimensi dan fokusnya, komponen kebijakan ruang siber terbagi menjadi tiga, yaitu (1) Komponen perdamaian dan keamanan internasional yang berfokus pada keamanan siber; (2) Komponen ekonomi, pembangunan, dan kejahatan yang berfokus pada keamanan data; dan (3) Komponen tata kelola internet yang berfokus pada pengaturan Internet (2018, hal. 14).

KEAMANAN SIBER (*CYBER SECURITY*)

Keamanan siber merupakan fokus dalam kebijakan ruang siber dari komponen perdamaian dan keamanan internasional. Konsep keamanan siber telah muncul cukup lama. Konsep ini muncul dalam agenda pasca-Perang Dingin sebagai tanggapan atas perbauran antara inovasi teknologi dan perubahan kondisi geopolitik (Hansen & Nissenbaum, 2009, hal. 1155). Menurut Nissenbaum (2005), keamanan siber pertama kali digunakan oleh para ilmuwan komputer pada awal tahun 1990-an untuk menekankan serangkaian ketidakamanan yang terkait dengan jaringan komputer, tetapi kemudian bergerak melampaui konsep teknis dari keamanan komputer ketika para pengusungnya mendesak bahwa ancaman yang muncul dari teknologi digital dapat memiliki efek sosial yang merusak (dalam Hansen & Nissenbaum, 2009, hal. 1155).

Isu-isu keamanan siber tentu saja berbeda dari isu-isu keamanan tradisional. Kim (2014) menyebutkan bahwa isu-isu keamanan siber tidak berada di ranah "politik internasional" di antara negara-negara yang bersaing dalam masalah keamanan tradisional; tetapi berada dalam ranah “politik antar-jaringan” yang asimetris di antara aktor-aktor yang kompleks. Menurutnya, isu keamanan siber berkembang di lingkungan yang kompleks serta mengandung *bugs* dan *holes*—yaitu, "*exploits*"–dan virus komputer serta *malware* digunakan secara aktif (Kim, 2014, hal. 346). Terkait dengan hal ini, Sekretaris Jenderal Persatuan Telekomunikasi Internasional (ITU) PBB, Dr Hamadoun Toure, memperingatkan bahwa perang dunia berikutnya dapat terjadi di ruang siber (Putra & Punzalan, 2013, hal. 267).

Ancaman di ruang siber juga sampaikan oleh McAfee. Raksasa keamanan internet global, McAfee dalam laporan kriminologi virtualnya di tahun 2007, *Cybercrime: The Next Wave*, mengidentifikasi tiga tren global yang muncul di ruang siber, yaitu (1) ancaman yang meningkat terhadap keamanan nasional dari spionase web; (2) ancaman yang meningkat terhadap layanan daring; dan (3) munculnya pasar untuk mencari kerentanan perangkat lunak (Putra & Punzalan, 2013, hal. 268). Kemudian, dalam laporannya di tahun 2008, *Cybercrime versus Cyberlaw*, McAfee menyoroti beberapa masalah seperti (a) pemerintah yang belum memberikan prioritas yang cukup untuk kejahatan siber; (b) tidak adanya rezim penegakan hukum transnasional untuk memerangi kejahatan siber sehingga menghambat kerja sama internasional; dan (c) penegakan hukum di tingkat nasional dan lokal tidak dilengkapi dengan baik untuk mengatasi meningkatnya kejahatan siber terutama dalam forensik digital dan pengumpulan bukti (Putra & Punzalan, 2013, hal. 268).

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (311-333) doi: 10.24198/padjir.v1i3.26241

Selain itu, keamanan di ruang siber juga menjadi perhatian para *scholar*. Menurut Kim (2014), ancaman siber terus berkembang, serta semakin mengaburkan domain antara sipil dan militer, aktor negara dan non-negara, dan bahkan aktor manusia dan non-manusia (dalam Kim, 2014, hal. 324). Domain keamanan siber, yang ancamannya masih bersifat virtual, sehingga belum dianggap nyata, adalah ranah persaingan dari banyak wacana (Rid, 2013 dalam Kim, 2014, hal. 336). Maka, sekuritisasi keamanan menjadi penting untuk mendefinisikan tentang keamanan siber, tantangan apa yang dihadirkannya, siapa yang menimbulkan ancaman, dari mana ancaman itu berasal, dan bagaimana mengurangi ancaman keamanan siber (Deibert 2002; Hansen dan Nissenbaum 2009 dalam Kim, 2014, hal. 336). Menurut Buzan, sekuritisasi isu-isu tertentu didasari oleh "penetapan intersubjektif dari ancaman eksistensial yang memiliki efek politik yang substansial." (Buzan et al., 1998, dalam Kim, 2014, hal. 336).

Saat ini, ruang siber tidak hanya didominasi oleh negara, tetapi juga aktor-aktor non-negara. Ruang siber tidak hanya menjadi arena untuk kegiatan bisnis dan sosial, tetapi juga lingkungan bagi kejahatan, peretasan, dan terorisme (Kim, 2014, hal. 324). Oleh karena itu, pemerintah, perusahaan swasta, dan aktor non-negara lainnya berusaha untuk mengembangkan kemampuan dalam mengamankan sumber daya dan aktivitas mereka di ruang siber (Kim, 2014, hal. 324). Para pembuat kebijakan luar negeri dan akademisi Hubungan Internasional juga berupaya untuk memahami karakteristik teknologi dan struktural ruang siber, yang berbeda dari isu-isu keamanan tradisional. Salah satu kunci untuk memahami besarnya potensi ancaman siber adalah dengan memahami karakter internet sebagai jaringan yang kompleks (Kim, 2014, hal. 324).

Kesadaran negara-negara akan ancaman di ruang siber semakin meningkat terutama setelah peristiwa 9/11. Menurut Latham (2003), peristiwa ini memicu perhatian lebih jauh terhadap komputer, teknologi informasi, dan keamanan, tak terkecuali pada masalah perlindungan infrastruktur digital, pengawasan elektronik, peretasan oleh teroris, dan internet sebagai platform jaringan untuk komunikasi lintas negara dan melawan negara (dalam Hansen & Nissenbaum, 2009, hal. 1155-1156). Di luar AS, rezim non-demokratis, yang paling mencolok adalah China, telah berulang kali berupaya untuk memblokir akses warga negara mereka ke bagian-bagian internet yang dianggap mengancam stabilitas politik dan sosial (Hansen & Nissenbaum, 2009, hal. 1156).

Upaya untuk meningkatkan keamanan siber di kawasan Asia Tenggara juga dilakukan oleh negara-negara anggota *Association of Southeast Asian Nations* (ASEAN). ASEAN telah mengambil langkah-langkah bersama untuk keamanan siber sejak tahun 2001 hingga saat ini. Wibisono mencatat pada tahun 2001 ASEAN membuat *e-ASEAN Framework Agreement* dan di tahun 2003 Singapura mendeklarasikan untuk membakukan *computer emergency response team* (CERT) (2018, hal. 8). Kemudian, ASEAN mengadakan komunike bersama *ASEAN Ministerial Meeting on Transnational Crime* (AMMTC) ke-4 pada tahun 2004, membuat program pengembangan kapasitas siber ASEAN di tahun 2016, dan membentuk Kelompok Kerja Ahli *ASEAN Defence Ministers Meeting* (ADMM) Plus untuk Keamanan Siber pada tahun 2017 (Wibisono, 2018, hal. 8). Selanjutnya, bersama dengan Jepang, ASEAN mendirikan pusat pengembangan kapasitas keamanan siber di Bangkok pada tahun 2018. Di tahun yang sama, ASEAN juga mengadakan Konferensi Tingkat Menteri ke-3 ASEAN tentang Keamanan Siber di Singapura untuk mendukung penerapan 11 norma internasional yang direkomendasikan oleh UN GGE pada tahun 2015 (Wibisono, 2018, hal. 8).

Wibisono juga mencatat ada beberapa tantangan yang dihadapi oleh ASEAN dalam

implementasi keamanan siber. Tantangan tersebut diantaranya adalah adanya disparitas dalam kemampuan siber dari negara-negara anggota ASEAN, baik dalam hal teknologi, operasional, kebijakan, maupun kapasitas hukum; representasi ASEAN di UN GGE Hanya diwakili oleh Malaysia dan Indonesia; dan adanya keengganan negara-negara anggota ASEAN terhadap isu keamanan politik yang kompleks (Wibisono, 2018, hal. 8).

Selain itu, pengamat politik mencatat bahwa telah terjadi peningkatan militerisasi ruang siber terutama sejak 9/11. Deibert misalnya, menunjukkan bahwa, dipicu oleh ketakutan akan potensi penggunaan jaringan elektronik oleh teroris dan "Pearl Harbor elektronik", negara-negara secara bertahap mengadopsi kemampuan perang informasi ofensif (dalam Putra dan Punzalan, 2013, hal. 270). Kemudian, serentetan serangan siber internasional pada tahun 2000-an, juga membuat isu keamanan siber mendapat perhatian yang lebih dari komunitas keamanan (Putra & Punzalan, 2013, hal. 272). Di negara-negara tertentu, isu keamanan siber telah diangkat ke level *high politics* dan angka-angka yang menonjol dalam agenda keamanan nasional serta arsitektur ICT (Putra & Punzalan, 2013, hal. 272). Kebijakan keamanan siber dirumuskan dengan maksud untuk mempertahankan integritas sistem informasi negara dan jaringan komunikasi, sementara badan keamanan siber nasional dalam permutasi yang berbeda dibuat untuk melembagakan kebijakan ini (Putra & Punzalan, 2013, hal. 272). Namun, ada juga unsur keamanan manusia di ruang siber yang harus dipertimbangkan dalam menganalisis implikasi keamanan siber (Putra & Punzalan, 2013, hal. 274). Negara bukan satu-satunya objek rujukan karena implementasi luas dari ICT telah membuat masyarakat menjadi bergantung pada produksi dan penyampaian informasi. Konsensus umumnya adalah bahwa ICT bertanggung jawab atas transformasi dari masyarakat industri ke masyarakat informasi. Akses ke informasi telah menjadi karakteristik utama dari masyarakat informasi (Putra & Punzalan, 2013, hal. 274).

Selain pendekatan tradisional, terdapat beberapa pendekatan non-tradisional untuk keamanan siber. Putra dan Punzalan mengemukakan tiga pendekatan non-tradisional untuk keamanan siber, yaitu Model Dualistik dari Keamanan Komputer Teknis dan Keamanan Siber, Model *Panopticon*, dan *E-governance*. Model pertama adalah Model Dualistik dari Keamanan Komputer Teknis dan Keamanan Siber. Nissenbaum mengilustrasikan konsepsi yang kontras dari keamanan komputer dan keamanan siber (Putra & Punzalan, 2013, hal. 278). Meskipun keduanya memiliki elemen yang sama, masing-masing model mengandung nilai yang berbeda. Sementara "keamanan komputer teknis" didefinisikan oleh tujuannya untuk memastikan ketersediaan informasi, integritas, dan kerahasiaan melalui perlindungan sistem komputer dan pengguna, "keamanan siber" didefinisikan oleh tujuannya untuk melindungi negara dari penggunaan jaringan komputer yang bertujuan subversif, serangan aktual pada infrastruktur sosial yang penting yang bergantung pada komputer, dan dari ancaman kerusakan jaringan (Putra & Punzalan, 2013, hal. 278). Model kedua adalah *Panopticon* yang bertujuan untuk pengawasan dan keamanan siber. Pada dasarnya, pembentukan rezim pengawasan membantu mengubah elemen-elemen dari "Model *Panopticon*" yang dibuat Bentham untuk mempertahankan disiplin dalam masyarakat itu sendiri (Putra & Punzalan, 2013, hal. 279). Sementara *Panopticon* dimaksudkan sebagai sistem untuk secara efisien menjaga pengawasan terhadap tahanan, model ini sekarang dapat digunakan untuk menggambarkan “rezim pengawasan kapitalis” modern (Putra & Punzalan, 2013, hal. 279-280). Model ketiga adalah *E-Governance* yang bertujuan untuk mengelola negara dan masyarakat di ruang Siber. *E-governance* didefinisikan sebagai penerapan sarana elektronik dalam interaksi antara pemerintah dan warga negara, pemerintah dan bisnis, serta dalam operasi internal pemerintah

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (311-333) doi: 10.24198/padjir.v1i3.26241

(Putra & Punzalan, 2013, hal. 282). Menurut Backus, *E-governance* digunakan untuk menyederhanakan dan memperbaiki aspek demokratis, pemerintah, dan bisnis dari *governance* (2001 dalam Putra & Punzalan, 2013, hal. 282).

Keamanan Data (Data Security)

Keamanan data merupakan fokus dalam kebijakan ruang siber dari komponen ekonomi, pembangunan, dan kejahatan. Keamanan data adalah seperangkat standar dan teknologi yang melindungi data dari kerusakan, modifikasi, atau pengeksposan baik yang disengaja maupun tidak disengaja (Forcepoint, t.t.). Keamanan data dapat diterapkan menggunakan berbagai teknik dan teknologi, termasuk kontrol administratif, keamanan fisik, kontrol logis, standar organisasi, dan teknik perlindungan lainnya yang membatasi akses ke pengguna atau proses yang tidak sah atau berbahaya (Forcepoint, t.t.).

Keamanan data penting karena semua kegiatan yang dilakukan pemerintah, bisnis, dan individu tidak lepas dari data. Data berperan di perusahaan baik besar maupun kecil, mulai dari raksasa perbankan yang menangani data pribadi dan keuangan dalam jumlah besar hingga bisnis kecil yang menyimpan detail kontak pelanggannya di ponsel (Forcepoint, t.t.). Elemen utama dari keamanan data adalah kerahasiaan, integritas, dan ketersediaan (CIA) (Buckbee, 2019). Kerahasiaan memastikan bahwa data hanya diakses oleh individu yang berwenang; integritas memastikan bahwa informasi dapat diandalkan dan juga akurat; dan ketersediaan memastikan bahwa data tersedia dan dapat diakses untuk memenuhi kebutuhan pengguna (Buckbee, 2019).

Tata Kelola Internet (Internet Governance)

Pengaturan internet merupakan fokus dalam kebijakan ruang siber dari komponen tata kelola internet. Internet adalah jaringan besar dari jaringan yang dikelola secara independen dan dirangkai oleh protokol komunikasi data berstandar global (terutama Protokol Internet, *Transmission Control Protocol* [TCP], *User Datagram Protocol* [UDP], Domain Name System [DNS], dan *Border Gateway Protocol* [BGP]) (Internet Governance Project, t.t.). Tata kelola Internet mengacu pada aturan, kebijakan, standar, dan praktik yang mengoordinasikan dan membentuk ruang siber global (Internet Governance Project, t.t.). Tugas utama dari tata kelola internet meliputi desain dan administrasi teknologi yang diperlukan untuk menjaga operasional internet dan pemberlakuan kebijakan substantif di seputar teknologi ini (DeNardis, 2014, hal. 6-7). Kelembagaan dan kerangka teknis tata kelola internet yang rumit berada di belakang layar dan tidak terlihat oleh pengguna (DeNardis, 2014, hal. 7). Tata kelola internet sebagian besar dilakukan oleh perusahaan swasta dan entitas nonpemerintah, misalnya dalam hal pengumpulan dan penyimpanan data industri periklanan *online*, mesin pencari, dan perantara informasi lainnya (DeNardis, 2014, hal. 12). Perusahaan swasta yang melakukan tata kelola internet terkadang juga bertindak sebagai aktor yang merespons peristiwa di panggung politik yang lebih besar, misalnya dengan menghentikan layanan ke WikiLeaks setelah WikiLeaks mengekspos korespondensi diplomatik yang sensitif (DeNardis, 2014, hal. 12).

Meski saat ini sudah banyak lembaga-lembaga yang melakukan tata kelola internet, pada awalnya internet tidak diatur dan sebagian besar tata kelolanya bersifat informal. *Stakeholder* utamanya bukanlah negara, tetapi para *engineer* dan internet berada di dalam ranah masyarakat dunia (Barrinha & Renard, 2017, hal. 358). Seiring berjalannya waktu, pemerintah menjadi lebih terlibat dan ruang siber lebih diatur, pertemuan internasional menjadi lebih banyak, yang membuka jalan bagi sejumlah besar forum baru tentang isu-isu siber (Barrinha & Renard, 2017, hal. 358). Beberapa pertemuan tersebut kemudian menjadi terstruktur dalam konteks organisasi

internasional, terutama PBB, yang meluncurkan *World Summit on the Information Society* (WSIS) pada tahun 2003, dengan delegasi dari 175 negara yang berpartisipasi, serta dalam beberapa organisasi regional, seperti Uni Eropa, *Organization for Security and Co-operation in Europe* (OSCE), Forum Regional ASEAN atau Dewan Eropa (Barrinha & Renard, 2017, hal. 358).

Lembaga-lembaga penting yang melakukan tata kelola internet, termasuk organisasi penetapan standar, diantaranya adalah ICANN, *World Wide Web Consortium* (W3C), *Internet Engineering Task Force* (IETF), *International Telecommunication Union* (ITU), *Institute of Electrical and Electronics Engineer* (IEEE), dan banyak lagi yang lainnya (DeNardis, 2014, hal. 22).

Gambar 1 berikut menunjukkan *timeline* dari tata kelola internet yang sudah berlangsung sejak Januari 1987 hingga Oktober 2016. Dalam *timeline* ini bisa kita lihat upaya pengaturan internet yang dilakukan oleh berbagai negara di masing-masing kawasan.

KESIMPULAN

Kemajuan teknologi informasi dan komunikasi memberikan banyak kemudahan dalam pelaksanaan aktivitas sehari-hari mulai dari pemerintah, bisnis, hingga individu. Kemudahan ini juga yang akhirnya membuat kita menjadi sangat tergantung pada teknologi. Ketergantungan ini kemudian memunculkan ancaman terhadap infrastruktur, proses politik, dan privasi individu. Selain itu, pertentangan karena konflik kepentingan antarnegara juga menimbulkan gesekan dalam hubungan internasional. Oleh karena itu, *cyber diplomacy* menjadi penting untuk meminimalkan gesekan, mencegah perang siber yang terbuka, dan mewujudkan penggunaan ruang siber yang damai.

Cyber diplomacy adalah praktik internasional yang muncul, atas upaya membangun masyarakat siber internasional, dengan menjembatani antara kepentingan nasional negara dan dinamika masyarakat dunia. Oleh karena itu, tujuan dari *cyber diplomacy* adalah untuk memenuhi fungsi-fungsi tradisional diplomasi, seperti menjaga perdamaian serta membangun rasa saling percaya di antara para pemangku kepentingan, di ruang siber. Hal ini sejalan dengan teori Diplomasi yang dikemukakan oleh para scholar dari mazhab *English School*. Bagi mazhab ini, diplomasi merupakan inti dari politik internasional; diplomasi adalah lembaga sentral dalam definisi dan pemeliharaan masyarakat internasional.

Menurut penulis, ada dua fungsi utama dari diplomasi untuk menciptakan perdamaian dalam masyarakat internasional, yaitu sebagai alat komunikasi internasional untuk membangun norma bersama dan sebagai upaya untuk meminimalkan gesekan dalam hubungan internasional. Jika dikaitkan dengan diplomasi dalam ruang siber, *cyber diplomacy* harus berfungsi sebagai alat komunikasi internasional untuk membangun norma siber bersama dan sebagai upaya untuk meminimalkan gesekan di ruang siber. Dengan dilakukannya fungsi tata kelola dan komunikasi dalam ruang siber global, penggunaan ruang siber yang damai dapat diwujudkan. Jadi, teori Diplomasi yang dikemukakan oleh mazhab *English School* dapat membantu menjawab pertanyaan utama penulis, "Apa yang dimaksud dengan *cyber diplomacy* dan apa yang bisa dijanjikannya bagi penggunaan ruang siber yang damai?"

Upaya untuk membangun norma siber bersama telah digagas oleh berbagai negara, organisasi internasional, dan perusahaan teknologi swasta, diantaranya adalah *NATO Talinn Manual*, *Microsoft Norms Paper*, *Code of* Conduct–yang digagas oleh China, Rusia dan negara lainnya–*US Government Policy*, dan *United Nations Group of Governmental Expert on Information Security* (UN GGE). Selain pembangunan norma, upaya untuk meminimalkan gesekan di ruang siber dapat dilakukan dengan mengembangkan kebijakan ruang siber internasional. Menurut Wibisono, jika dilihat dari dimensi dan fokusnya, komponen kebijakan ruang siber terbagi

e-ISSN: 2684-8082 Vol. 1 No. 3, Januari 2020 (311-333) doi: 10.24198/padjir.v1i3.26241

menjadi tiga, yaitu (1) Komponen perdamaian dan keamanan internasional yang berfokus pada keamanan siber; (2) Komponen ekonomi, pembangunan, dan kejahatan yang berfokus pada keamanan data; dan (3) Komponen tata kelola internet yang berfokus pada pengaturan internet (Wibisono, 2018, hal. 14).

DAFTAR PUSTAKA

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs, 3*(4-5), 353-364. doi:10.1080/23340460.2017.1414924

Bjola, C. (2015). Introduction: Making sense of digital diplomacy China. Dalam C. Bjola, & M. Holmes (Penyunt.), *Digital diplomacy: theory and practice*. New York: Routledge.

Bjola, C., & Jiang, L. (2015). Social Media and Public Diplomacy: A comparative analysis of the digital diplomatic strategies of the EU, US and Japan in China. Dalam C. Bjola, & M. Holmes (Penyunt.), *Digital diplomacy: theory and practice*.

Bjola, C., & Pamment, J. (2019). Introduction: The 'dark side' of digital diplomacy. Dalam C. Bjola, & J. Pamment (Penyunt.), *Countering online propaganda and extremism: the dark side of digital diplomacy*. New York: Routledge.

Buck, S. J. (1998). *The global commons: An introduction*. Washington DC: Island Press.

Buckbee, M. (2019). *Data Security: Definition, Explanation and Guide*. Retrieved December 20, 2019, from https://www.varonis.com/blog/data-security/

Bull, H. (1977). *The anarchical society: A study of order in world politics* (2nd ed.). Houndmills, UK: Macmillan.

CCD COEa. (t.t.). *21 Top International Law Experts Discuss Tallinn Manual 2.0 (Video)*. Retrieved December 17, 2019, from https://ccdcoe.org/news/2015/21-top-international-law-experts-discuss-tallinn-manual-2-0-video/

CCD COEb. (t.t.). *Tallinn Manual 2.0*. Retrieved December 17, 2019, from https://ccdcoe.org/research/tallinn-manual/

Chansoria, M. (2012). Defying Borders in Future Conflict in East Asia: Chinese Capabilities in Therealm of Information Warfare and Cyber Space. *The Journal of East Asian Affairs, 26*(1), 105-127.

Cresswel, J. W. (2013). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. Sage Publications.

DeNardis, L. (2014). *The Global War for Internet Governance*. Yale University Press.

Djajasudarma, F. (2009). *Metode linguistik: ancangan metode penelitian dan kajian*. Bandung: Refika Aditama.

Forcepoint. (t.t.). *What is Data Security?* Retrieved December 20, 2019, from https://www.forcepoint.com/cyber-edu/data-security

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155-1175.

Heffter, A., & Goel, S. (2018). Mitigating Cyber Warfare through Deterrence and Diplomacy. *The 13th Pre-ICIS Workshop on Information Security and Privacy, December 13, 2018*. San Francisco.

Hodzic, N. (2017). *Cyber-Diplomacy: Framing the Transformation*. Thesis, Central European University, Department of International Relations , Budapest, Hungary.

Internet Governance Project. (t.t.). *What is Internet Governance?* Retrieved December 17, 2019, from https://www.internetgovernance.org/what-is-internet-governance/

Kim, S. (2014). Cyber Security and Middle Power Diplomacy: A Network Perspective. *The Korean Journal of International Studies, 12*(2), 323-352.

Manor, I., & Segev, E. (2015). America's Selfie: How the US portrays itself on its social media accounts. Dalam C. Bjola, & M. Holmes (Penyunt.), *Digital diplomacy: theory and practice*. New York: Routledge.

McKune, S. (2015). *An Analysis of the International Code of Conduct for Information Security*. Retrieved December 17, 2019, from https://citizenlab.ca/2015/09/international-code-of-conduct/

Putra, N. A., & Punzalan, K. (2013). Cyber security. Dalam M. Caballero-Anthony, & A. D. Cook (Penyunt.), *Non-Traditional Security in Asia: Issues, Challenges and*

Framework for Action. ISEAS–Yusof Ishak Institute.

Roche, E. M. (2019). The search for global cyber stability. *Journal of Information Technology Case and Application Research*, *21*(2), 68-73. doi:10.1080/15228053.2019.1636570

Schmitt, M. N. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations* . New York: Cambridge University Press.

Sotiriu, S. (2015). Digital Diplomacy: Between promises and reality. Dalam C. Bjola, & M. Holmes (Penyunt.), *Digital diplomacy: theory and practice*. New York: Routledge.

U.S. Department of State. (2015). *An Open and Secure Internet: We Must Have Both*. Retrieved December 17, 2019, from https://2009-2017.state.gov/secretary/remarks/2015/05/242553.htm

UNODA Fact Sheet. (2019). *Developments in the Field of Information and Telecommunications in the Context of International Security*. UNODA.

UNODA. (t.t.). *Developments in the field of information and telecommunications in the context of international security*. Retrieved December 24, 2019, from UN Office for Disarmament Affairs: https://www.un.org/disarmament/ict-security/

Watson, A. (1984). *Diplomacy: The dialogue between states*. London: Methuen.

Wibisono, A. A. (2018). *Kebijakan Kawasan Siber Asean – Polarisasi UNGGE*. National Think Tank on Cyber Diplomacy.

Wight, M. (1979). *Systems of states*. Leicester: Leicester University Press.

BIOGRAFI

Iskandar Hamonangan, Program Pascasarjana Departemen Hubungan Internasional Universitas Indonesia. Keterarikan (*area of interest*) dalam studi Hubungan Internasional meliputi *Transnational Relations Studies*, *Diplomacy Studies*, *Foreign Policy Studies*, *Non-Traditional Security Studies*, *Globalization* dan *Human Rights & Democracy Studies*.

Zainab Assegaff, Program Pascasarjana Departemen Hubungan Internasional Universitas Indonesia. Keterarikan (*area of interest*) dalam studi Hubungan Internasional meliputi *International Political Economic Studies*, *Diplomacy Studies*, *Development Studies*, *Globalization* dan *Non-Traditional Security Studies*.